(U) VALIANTSURF

From WikiInfo

(TS//SI//REL) **VALIANTSURF** is the coverterm for the development of Data Network Cipher (DNC) exploitation capabilities in TURMOIL for integration into the TURBULENCE DNC thread. VALIANTSURF is the preferred reference for all TURBULENCE DNC exploitation capabilities since the fact that NSA does work with DNC's is classified "S//REL". The TURBULENCE DNC capability exploits communications encrypted with DNC Internet Protocols.

Contents

(U) Data Network Cipher (DNC) Classification

(U) Official CES Classification Guide

- (U//FOUO) CES CRYPTANALYSIS 02-12 ([redacted]
- (U//FOUO) CLASSIFICATION GUIDE FOR ECI PICARESQUE (PIQ) 02-10 ([redacted]

(U) Guidelines

- (U//FOUO) The fact that NSA is interested in DNC is U//FOUO.
- (S//REL) Just the fact that NSA does work with DNC is classified.
  - (S//REL) If the only information given is that you are a DNC expert or you work on DNCs, then the classification is S//REL
  - (TS//SI//ORCON/REL) If the information given is that you decrypt DNCs, the classification is, at a minimum TS//SI //ORCON//REL
  - (TS//SI//ORCON/REL) If the fact of DNC exploitation is mentioned or inferred (with or without mention of a specific target or person), the classification is TS//SI//ORCON//REL
  - (TS//SI//ORCON/REL) The decryption results are classified, at a minimum, TS//SI//REL

(TS//SI//ORCON/REL) The classifications above are the minimum classifications. A higher classification may be required depending on the rest of the content. For example, mentioning you work on DNCs is SECRET//REL but if you mention you work on DNCs and are in CES, the classification should be TS//SI//ORCON//REL since CES deals with exploitation.

(U) DNC Protocols

(U) IPsec

(U) The IPsec DNC protocol suite comprises the following protocols:

File:DNC IPSEC Operation.jpg
(U) IPsec DNC Operation

- (U) ISAKMP – Internet Security Association and Key Management Protocol (RFC 2407, RFC 2408) provides an authentication and key exchange framework.
- (U) IKE – Internet Key Exchange v1(RFC 2409) and v2(RFC 4306) provide an authentication and key exchange mechanism.
- (U) ESP – Encapsulating Security Payload (RFC 2406) provides traffic confidentiality (via encryption) and optionally provides authentication and integrity protection.
- (U) AH – Authentication Header (RFC 2402) provides integrity and authentication protection the includes immutable IP header fields. This differs from ESP integrity protection that does not include the IP header.

(U) PPTP

(U) The Point-to-Point Tunneling Protocol (PPTP) was developed in 1996 by the PPTP Forum, comprised of Ascend Communications, U.S. Robotics, 3Com, Copper Mountain Networks, ECI Telematics, and lead by Microsoft.

(U) The Microsoft implementation of PPTP (RFC 2637) permits the data link layer protocol, Point-to-Point Protocol (PPP) (see STD-0051), to be tunneled through an IP network, encapsulated within an enhanced/modified Generic Routing Encapsulation (GRE) transport protocol (IP Next Protocol 47). The contents of the PPP data is normally IP network protocol packets for a private network, but can also carry any other Local Area Network (LAN) protocol, like Microsoft NetBEUI or Novell IPX/SPX.

(U) Microsoft PPTP (MS-PPTP) permits the encapsulated PPP data to be authenticated using either version 1 (RFC 2433) or version 2 (RFC 2759) of the Microsoft extensions to the PPP Challenge Handshake Authentication Protocol (CHAP) (RFC 1994), and to be encrypted using RC4 with key lengths of 40, 56, or 128 bits (RFC 3078, RFC 3079). The mode of the encryption is negotiated and key lengths are exchanged using the PPP Compression Control Protocol (CCP) (RFC 1962).

(U) HOOKED

(TS//SI//REL) HOOKED HAND is a DNC protocol used in a commercial DNC product.

(U) CINDER

(TS//SI//REL) CINDERASH/TRACK are ESP-like protocols that use non-RFC defined fields.

(U) DNSC

(TS//SI//REL) DNSC is ...

SCARLETFEVER SSL Brief

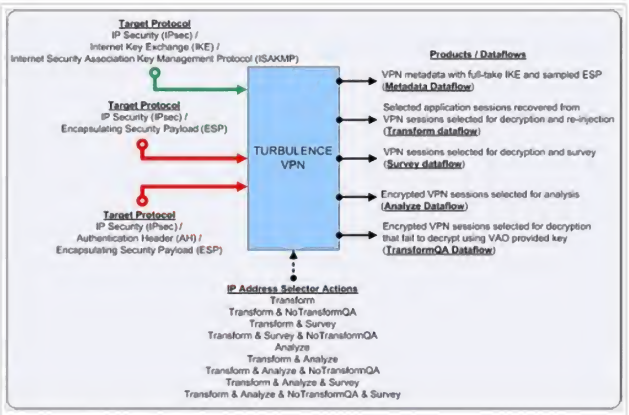
(U) TU DNC Products

(S//SI//REL) IPSec DNC Products

(S//SI//REL) The TU DNC products are the outputs of four processing data flows:

- (S//SI//REL) The TU DNC Metadata flow collects metadata about IPsec (IKE/ISAKMP and ESP) events then forwards the metadata to follow-on SIGINT Development (SIGDEV) systems.
- (TS//SI//REL) The TU DNC Decryption flow detects IPsec communications, selects by IP-Address, decrypts the traffic selected for decryption, and re-injects the encapsulated (cleartext) content into TURMOIL for processing.

- (TS//SI//REL) The TU DNC Survey flow forwards to XKEYSCORE all encapsulated (cleartext) sessions that are selected by IP-Address for decryption by the TU DNC Decryption flow that are also marked for SIGDEV.
- (S//SI//REL) The DNC Analyze flow selects by IP-Address IKE/ISAKMP and ESP packets that are then sessionized and forwarded to PRESSUREWAVE for analysis.



(TS//SI//REL) TU VPN Products

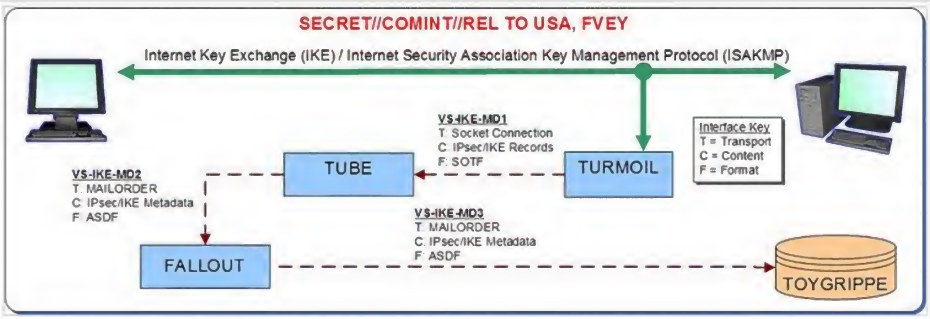
(U) Spin History

(TS//SI//REL) Spin 9 efforts transitioned fielded DNC software from the Red TURMOIL (TML) architecture to the Blue and implemented a redesign of the decryption flow that reallocates some functionality between TURMOIL and the DNC Attack Orchestrator (VAO).

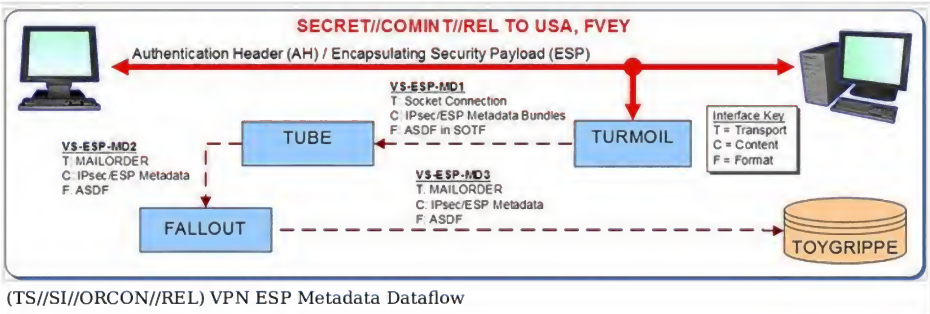
(TS//SI//REL) Spin 10 efforts started development of a decryption capability that can be deployed to SMK, improved DNC detection and processing capabilities, and developed the DNC Analyze flow.

(S//SI//REL) DNC Metadata Flow

- (TS//SI//ORCON//REL) The DNC Metadata Flow collects metadata about IKE/ISAKMP and AH/ESP events and forwards the metadata to follow-on SIGINT Development (SIGDEV) systems.
- (TS//SI//ORCON//REL) All IKE/ISAKMP packets seen in the incoming data are collected, bundled and then sessionized within TURMOIL. Then the metadata is extracted, converted to ASDF and then sent to the ASDFReporter component within TURMOIL. The ASDFReporter gathers all ASDF generated within TURMOIL and sends the bundles to FALLOUT via TUBE. FALLOUT delivers the metadata records to the appropriate destinations. The IPSec IKE metadata all goes to TOYGRIPPE via MAILORDER. TOYGRIPPE is a DNC analytic database in CES used by the cryptanalysts in conjunction with a vulnerability database to determine exploitability.
- (TS//SI//ORCON//REL) Sampled AH/ESP packets seen in the incoming data are collected, metadata is extracted per session, and the metadata is converted to ASDF and sent to the ASDFReporter within TURMOIL. The ASDF records follow the same paths as the IKE Metadata above.



(TS//SI//ORCON//REL) VPN IKE Metadata Dataflow



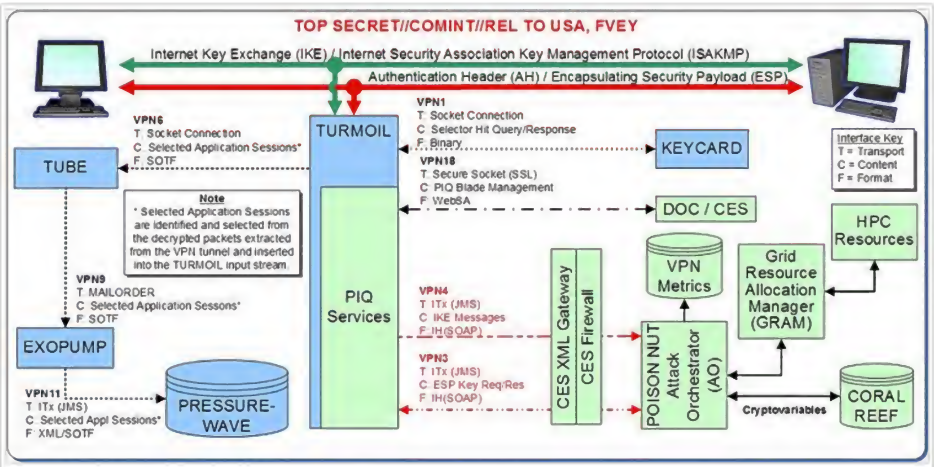
(TS//SI//ORCON//REL) VPN ESP Metadata Dataflow

(TS//SI//ORCON//REL) DNC Decryption Flow

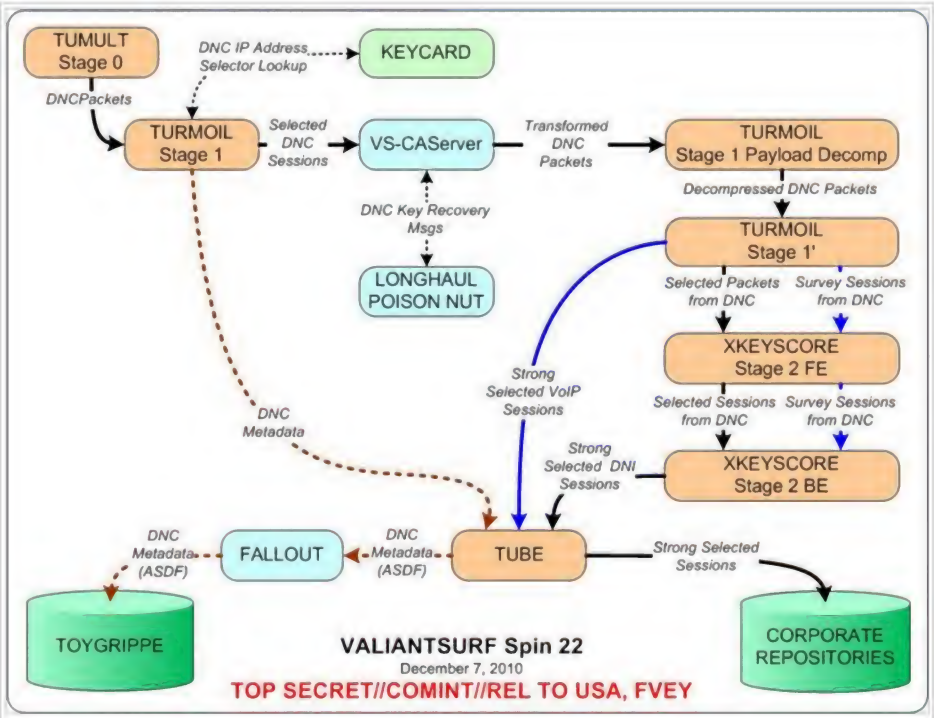
- (TS//SI//ORCON//REL) The DNC Decryption Flow detects and decrypts selected communications that are encrypted using IPsec then reinjects the unencrypted packets back into TURMOIL Stage 1. TURMOIL Stage 1 applications process the packets into sessions and when appropriate forwards the unencrypted content to follow-on processing systems. The DNC eventing (PPF) components in TURMOIL detect all IKE/ISAKMP and ESP packets and queries KEYCARD for each unique IKE exchange session and each unique ESP session to determine if the link should be selected for processing. Selection is based on IP address. Decryption is attempted if either the source or the destination IP address is targeted for decryption in KEYCARD (the KEYCARD tasking action is labeled "TRANSFORM" so as not to use the term "decrypt"). If KEYCARD returns a hit for an IKE packet, then the IKE packet is sent to LONGHAUL where is is used to recover keys. If KEYCARD returns a hit for an ESP packet, a key request is sent to LONGHAUL. The IPsec Security Parameter Index (SPI) correlates IKE

sessions with ESP sessions. A LONGHAUL response message will either return the key or indicate that a key could not be recovered. If a key is recovered, the ESP packets are decrypted and re-injected into TURMOIL for further processing.

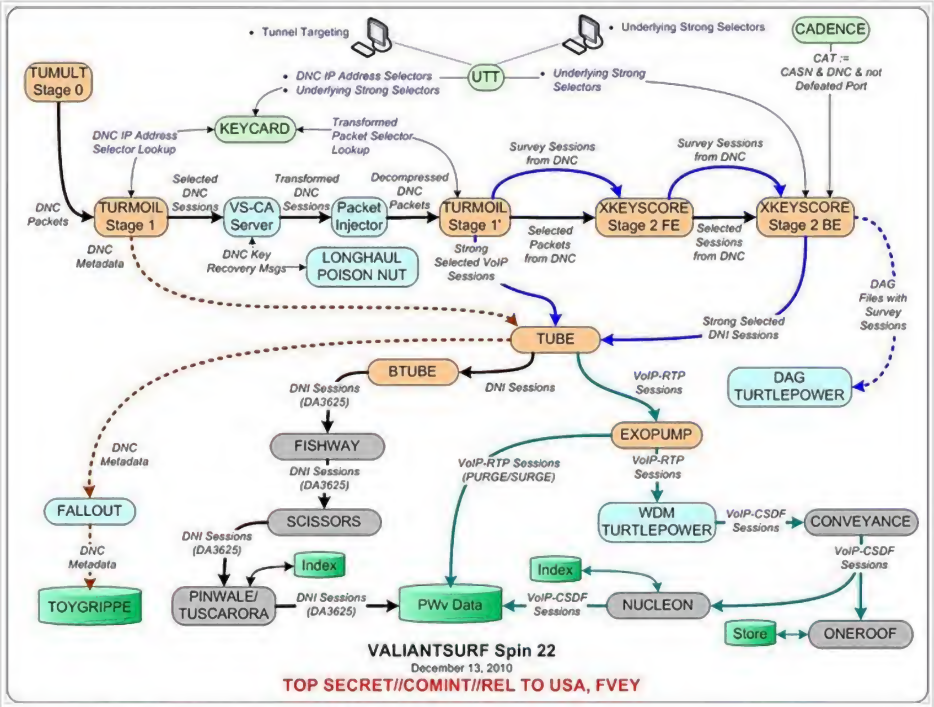
- (TS//SI//ORCON//REL) All DNC Decryption functions and communications with LONGHAUL, specifically POISONNUT, the Attack Orchestrator (and a DNC Metrics service via POISONNUT) are hosted on a specially configured and dedicated TURMOIL processing host called a CA Server. All CA Service blade software is loaded and administered by CES approved and CA Services authorized administrators. The CA server is firewalled and effectively functions as an extension of the CES enclave. In the future all communications between the CA Server and the CES services (LONGHAUL, DNC Metrics) will be a secure JMS messaging service based on the ISLANDTRANSPORT / ISLANDHIDEAWAY infrastructure.



(TS//SI//ORCON//REL) VPN Decryption Dataflow

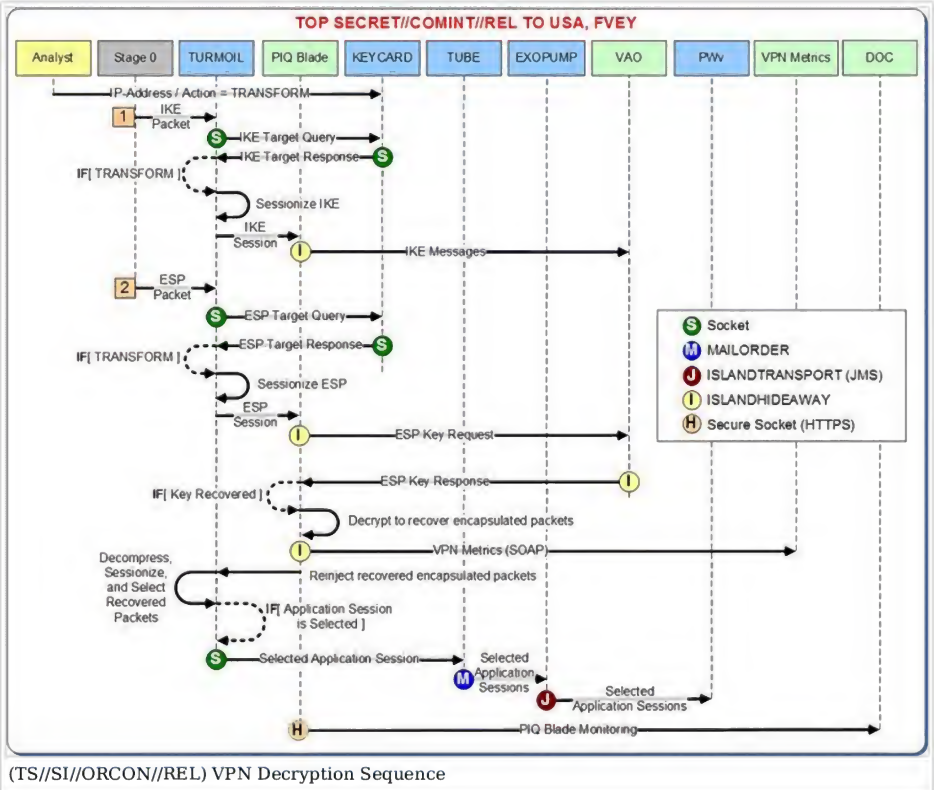


(TS//SI//ORCON//REL) Simple VALIANTSURF Dataflow

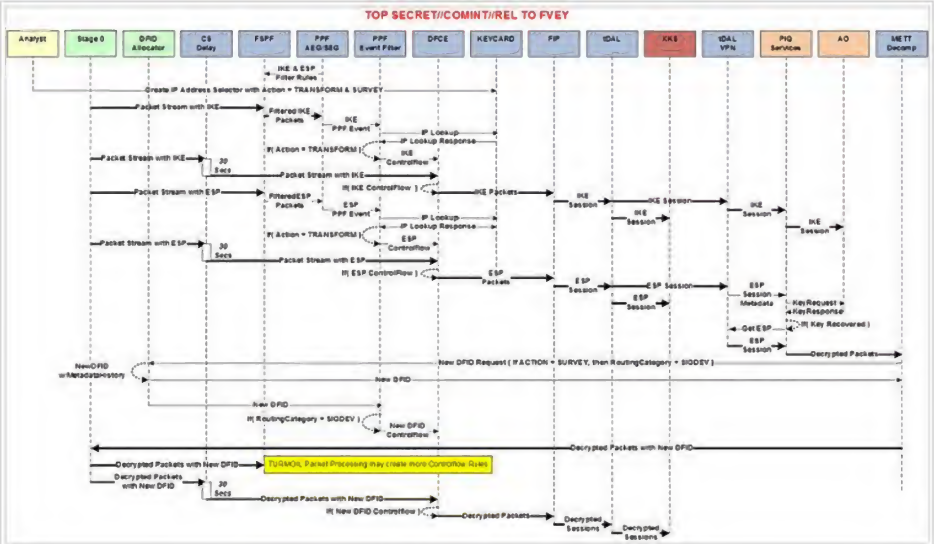


(TS//SI//ORCON//REL) Complex VALIANTSURF Dataflow

DEPRECATED



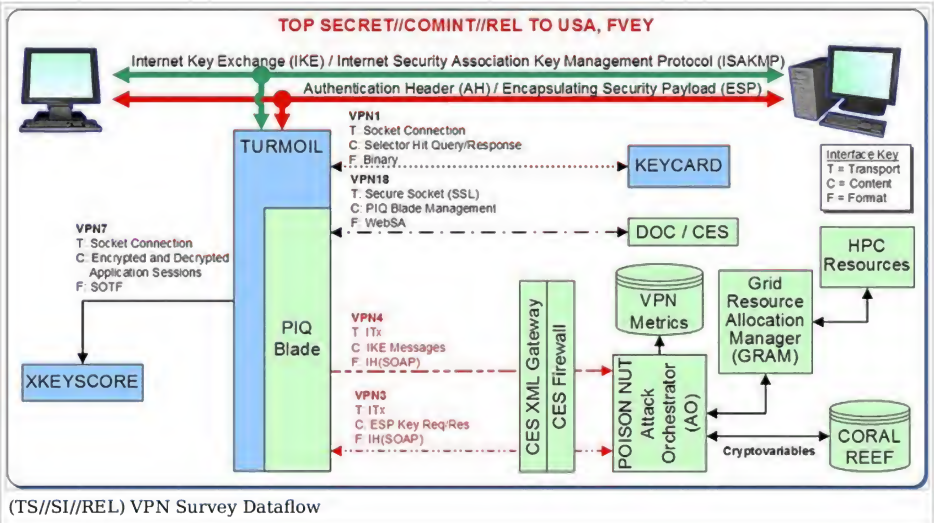
(TS//SI//ORCON//REL) VPN Decryption Sequence



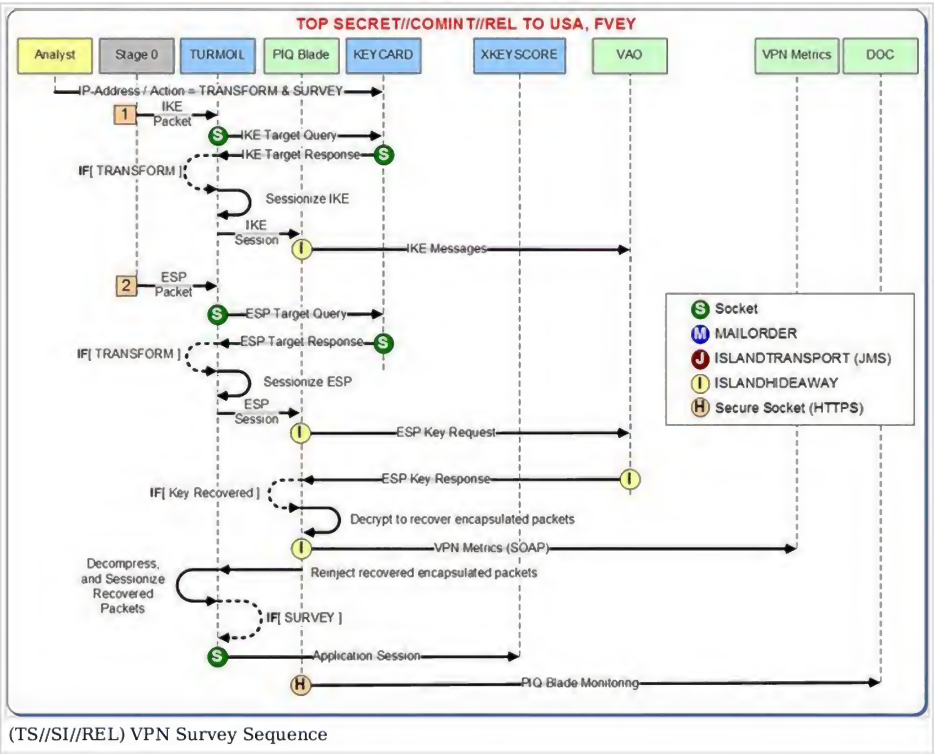
(TS//SI//ORCON//REL) Detailed Turmoil DNC Decryption Sequence Diagram

(TS//SI//REL) DNC Survey Flow

- (TS//SI//REL) The DNC Survey Flow detects, decrypts selected communications that are encrypted using IPsec; then sessionizes the unencrypted packets and sends the sessions to XKEYSCORE. The DNC eventing (PPF) components in TURMOIL detects all IKE/ISAKMP and ESP packets and queries KEYCARD for each unique IKE exchange session and each unique ESP session to determine if the link should be selected for processing. Tasking is based on IP address. Decryption is attempted if either the source or the destination IP address is tasked for decryption in KEYCARD (the KEYCARD tasking action is labelled "TRANSFORM" so as not to use the term "decrypt"). If KEYCARD returns a hit for an IKE packet, then the IKE packet is sent to the POISONNUT(DNC Attack Orchestration) Service. If KEYCARD returns a hit for an ESP packet, a key request is sent to POISONNUT. A POISONNUT response message will either return the key or indicate that a key could not be recovered. If a key is recovered, the ESP packets are decrypted and re-injected into TURMOIL for sessionization. If KEYCARD also associated a "SURVEY" action with the DNC Tunnel IP-Address the encapsulated sessions are sent to XKEYSCORE. The DNC Survey flow requires that both "TRANSFORM" and "SURVEY" actions are assigned to a targeted IP-Address.
- (TS//SI//REL) All DNC Decryption functions and communications with POISONNUT(and a DNC Metrics service) are hosted on a specially configured TURMOIL processor called a CA Server. All CA Server software is loaded and administered by CES approved and CA Server authorized administrators. The CA Server is firewalled and effectively functions as an extension of the CES enclave. In the future all communications between the CA Server and the CES services (POISONNUT, DNC Metrics) will use a secure JMS messaging service based on the ISLANDTRANSPORT/ ISLANDHIDEAWAY infrastructure.



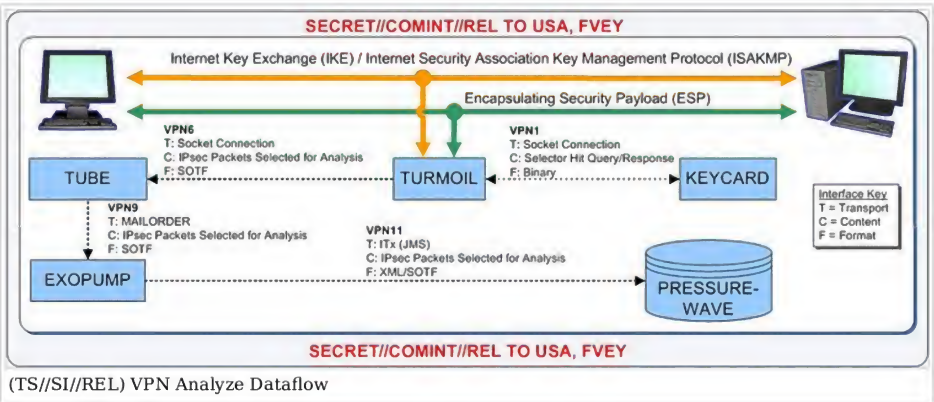
(TS//SI//REL) VPN Survey Dataflow



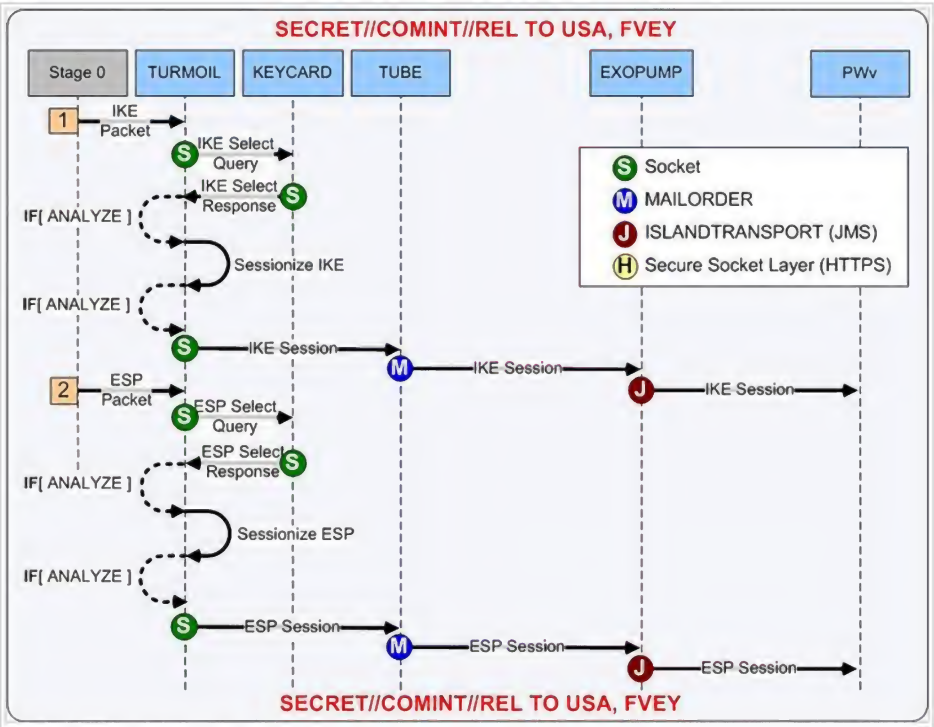
(TS//SI//REL) VPN Survey Sequence

(S//SI//REL) DNC Analyze Flow

- (TS//SI//REL) The DNC Analyze Flow selectively collects IKE/ISAKMP packets and raw, encryted ESP packets that are sessionized and forwarded to PRESSUREWAVE for analysis. The DNC eventing (PPF) components in TURMOIL detect all IKE/ISAKMP and ESP packets and queries KEYCARD for each unique IKE exchange and each unique ESP session to determine if the link should be selected for analysis. Tasking is based on IP address. If KEYCARD returns an "ANALYZE" action for any IPsec packet hit, then the IPsec packet is sessionized and sent to PRESSUREWAVE.



(TS//SI//REL) VPN Analyze Dataflow



(TS//SI//REL) VPN Analyze Sequence

(U) Requirements, Planning, and Reviews

(U) Design Details

(S//SI//REL) Architectural Taxonomy

- DNCA (Digital Network Crypt Applications) – branch
- ROMULANALE – Name of project within DNCA that develops capabilities for the CAServer
- GALLANTWAVE – DNSC project *and* thread on fielded systems, including TURMOIL and XKS (DeepDive)
  - GW Mission App – legacy capability on CAServer for DNSC decryption
  - ROMULANGAWK – ROMULANALE provided capability on CAServer for DNSC decryption in software
  - ROMULANGOWL – ROMULANALE provided capability on CAServer for DNSC decryption in hardware (pending)

- VALIANTSURF – DNC project *and* thread on fielded systems, currently including only TURMOIL
  - MALIBU – DNC processing architecture for VALIANTSURF on TURMOIL using session based processing
    - PIQServices – capability on CAServer for DNC decryption under MALIBU
  - WAIMEA – DNC processing architecture for VALIANTSURF on TURMOIL using packet stream based processing. This covers all configurations of the architecture (software and hardware)
    - WAIMEAVISAGE – DNC WAIMEA processing architecture with decryption performed in software
      - ROMULANVISAGE – ROMULANALE provided capability on CAServer for WAIMEAVISAGE
    - WAIMEAVISE – DNC WAIMEA processing architecture with decryption performed in hardware
      - ROMULANVISE – ROMULANALE provided capability on CAServer for DNC WAIMEAVISE

(U//FOUO) Current DNC Design Documents

- MALIBU Architecture
- WAIMEA Architecture

(U) Design Reviews and Technical Exchanges

(U) Technical Documents

- (S//SI//REL) IPsec Sessionization
- (S//SI//REL) HOOKED Sessionization
- (S//SI//REL) CINDER Sessionization
- (S//SI//REL) PPTP Sessionization
- (S//SI//REL) New Protocol (IPsecESP,PPTP,HOOKED,CINDER) Specification
- (TS//SI//REL) Turmoil Analysis for Increment 3
- (TS//SI//REL) VPN IKE ASDF data flow
- (TS//SI//REL) VPN IKE ASDF Sequence Diagram
- (TS//SI//REL) APEX\VPN Data Flow
- (TS//SI//REL) APEX\VPN Sequence Diagram

- (TS//SI//REL) Turmoil VPN Decrypt Sequence Diagram

- (TS//SI//REL) SPIN 15 VPN Story1
- (TS//SI//REL) Spin 15 TURMOIL Model
- (TS//SI//REL) S31322 Branch VPN Brief
- (TS//SI//REL) VS Monitoring

(U) DNC Enterprise Messaging Fabric

- (S//SI//REL) VPN AMF(ITx)Fabric Diagram

(S//SI//REL) DNC IKE SMG (Replaced Ike Analytic)

- (S) Description – The IKE SMG (Sesionized Metadata Generator) inherited the internal business logic of the IKE Analytic, but was re-hosted as an iBridge service. There is no longer any connection to PRESSUREWAVE or METROTUBE. The IKESMG runs as a CCM graph IPSEC_IKE_MDATA with input from IPSEC_EVENT_TO_BME via IOPort.
- (S) Spin 17 – No Release. Initial version developed but not delivered to TURMOIL
- (S) Spin 18 – Initial Release. Patched Version had verbose logging.
- (S) Core 3.1 – Part of ValiantSurf Shark feather. APEX processing removed. Sessionization by Exchange introduced.
- (S) Core 4.x – Future release compliant with Schema version 8.

(S//SI//REL) DNC IKE Analytic

- (S) Spin 15 – No Release. Verified Spin 14 VIAS runs successfully on Metrotube 2.3.1 (Metrotube Spin 15 version).
- (U) Other Wiki Links:
  - (U[redacted]S31321(CON) Analytic Developer
  - (S) **VALIANTSURF Wiki**
  - (S) VPN Metadata Flow diagram
  - (S) VpnIpsecVpnLargeDataCharacterization
- (S) Spin 14 – Upgraded Spagic workflow to follow the robust PWV Retriever Pattern.
  - (S) Pattern Comprises separate service assemblies for Listener, Metadata Retriever, DataRetriever, Throttler, and DNC wrapper.
  - (S) Error handling and VIAS logging capabilities added.
- (S) APEX (DEMO) – Modified SOTF Parser and TGIF Record Factory to process Apex metadata.
- (S) Spin 13 – Upgraded Spagic workflow to match Metrotube 2.1.
  - (S) Numerous bug fixes relating to Toygrippe content including Exchanges Types, Message Types, Phase2-Only, missing transforms(see MadForge DNC-analytic project for details).
  - (S) Added capability to process Toygrippe file classification determined by DNC Metadata.
- (S) Spin 12 – The VPN Analytic has been re-named as the VIAS (VPN IKE Analytic Service). In this spin, there were 2 major changes.
  - (S) First, the analytic was converted to run in the Metrotube 2 framework, as a JSorcerer Service on the Metrotube Service Bus.
  - (S) Second, the VIAS is now released by the ValiantSurf (DNC) team directly to Turbulence, where Spin 11 and earlier versions were packaged by the DNC team, delivered informally to Metrotube Services who performed the software release to Turbulence.
- (S) Spin 11 and prior – VPN Analytic runs as a Metrotube 1 service.
  - (S) An improvement to the IkeSessionizer algorithm correctly matched up the initiator and responder by waiting for the responder to return a non-ZRC (Zero Responder Cookie).

(U) CIET Tasking

- (S//SI//REL) Tasking for TEC/MHS/CROSSCUT

(U) Test

VALIANTSURF/TestData

- (S//SI//REL) RFCs Required for TML 18.1 and earlier releases
- (S//SI//REL) VALIANTSURF RFCs

(S//SI//REL) DNC Metadata

- (S//SI//REL) Spin14 VPN IKE Metadata Test Document
- (S//SI//REL) Spin13 VPN IKE Metadata Test Document
- (S//SI//REL) Spin12 VPN IKE Metadata Test Document

(TS//SI//REL) DNC Decrypt

- (TS//SI//REL) Spin12 VPN Decrypt Test Document

(U//FOUO) LONGHAUL Test

LONGHAUL Test Documentation Page

(U//FOUO) One CA Server Toggled among Multiple TURMOILs

(U//FOUO) This section describes a network design to have one CA server serve multiple TURMOILs. Note that a CA Server can only communicate to one TURMOIL at a time.

Motivation:

1. Power/space/cooling limitations
2. Long lead time to gain approval to add CA Services servers
3. Hardware cost
4. Limits on public IP address space at some sites

Click for details on the CA Server Bank.

For more information, Contact one of these POCs

[redacted] TML Network Engineer
CA Services Developer
TML Integration and Test
TURMOIL Lab Manager
T1 VS Thread Lead

(U) Deployments

VALIANTSURF Deployment Roles & Responsibilities
(U) CIET Deployment Overview
(U) VALIANTSURF Levels of Success

(U//FOUO) VALIANTSURF RFC and DR Needs for TURMOIL Baseline Deliveries 2011

(U//FOUO) VALIANTSURF RFC and DR Needs for TURMOIL Baseline Deliveries 2010

- (TS//SI//ORCON/REL) RFC DR Needs TURMOILBaselines

(U//FOUO) Live Dataflow

TU FLE VPN Metadata Beacons [redacted]

(U//FOUO) TURMOIL Installations

```
* RPM Log [redacted]
* Config Log [redacted]
```

(U//FOUO) IPsec/IKE Metadata Routing

Site	SIGAD	TUBE MAILORDER PDDG	TUBE MAILORDER Trigraph	TUBE MAILORDER System Digraph	System	Route	METROTUBE MAILORDER PDDG	ME MA Trig
MHS LATTICE	USJ-759	AH	HXN	51	MHS-LIVE-T16	via NSAW	OO	TYG
		KY	EXM	52	MHS-DEV-T16	via NSAW	OO	TYG
		N/A	N/A	N/A	MHS-DEV-T16	via Site Store	KY	TYG
MHS-STARQUAKE	USJ-759A	AH	HXN	51	MHS-LIVE-T16	via NSAW	OO	TYG

		KY	EXM	52	MHS-DEV-T16	via NSAW	OO	TYG
		KY	TYG	QX	MHS-DEV-T16	via Site Store	N/A	N/A
	US-3150	RU	EXN	51	G1-T16	via NSAW	OO	TYG
			DVN	52	G2-DEV-T16	via NSAW	OO	TYG
			LPN	53	G3-LPT	via NSAW	OO	TYG
			LPN	54	G4-LPT	via NSAW	OO	TYG
			LPN	55	G5-LPT	via NSAW	OO	TYG
			DVN	56	G6-DEV-LPT	via NSAW	OO	TYG
TEC	USD-1001TEC	BL	EXM	51	TEC-T16	via NSAW	OO	TYG
YRS	USF-787	MH	EXM	51	YRS3-LPT	via NSAW	OO	TYG

(U//FOUO) IPsec/ESP Metadata Routing FALLOUT to TOYGRIPPE

FALLOUT Processing & Dataflow
FALLOUT Dataflow Statistics [redacted]

Site	SIGAD	FALLOUT MAILORDER PDDG	FALLOUT MAILORDER Trigraph	TOYGRIPPE MAILORDER Trigraph	FALLOUT MAILORDER System Digraph	TUBE Upstream Source System Digraph (Source System Atom)	Upstream Source System
MHS-LATTICE	USJ-759	AH	KLG	TYF	D0,D9	51	MHS-LIVE-T16
				TYF	D0,D9	52	MHS-DEV-T16
MHS-STARQUAKE	USJ-759A	KY	KLG	TYF	D0,D9	51	MHS-LIVE-T16
				TYF	D0,D9	51	MHS-DEV-T16
	US-3150	RU	KLG	TYF	D0,D9	51	G1-T16
				TYF	D0,D9	52	G2-T16
				TYF	D0,D9	53	G3-LPT
				TYF	D0,D9	54	G4-LPT
				TYF	D0,D9	55	G5-LPT
				TYF	D0,D9	56	G6-LPT
TEC	USD-1001TEC	BL	KLG	TYF	D0,D9	51	TEC-T16
CROSSCUT	US-3301	U6	KLG	TYF			
SARATOGA	US-3167	IL	KLG	TYF			
MUSCULAR	DS-200B	C4	KLG	TYF			
YRS	USF-787	MH	KLG	TYF	D0,D9	51	YRS1-LPT
				TYF	D0,D9	52	YRS2-LPT
				TYF	D0,D9	53	YRS3-LPT

(S//SI//REL) VAO STATUS

POISONNUT Wiki

- Last Updated *Wed Mar 5 20:36:00 GMT 2008*
- *RUNNING*

(U//FOUO) Deployments and Development systems

(U//FOUO) VALIANTSURF TURMOIL components are deployed directly to the TURMOIL systems.

(U//FOUO) The VALIANTSURF mission-application is deployed on the CAServer platform. See CAServer#Deployments for site specific configuration.

(U//FOUO) CIET Deployments

Site	Type	Current TURMOIL	Next TURMOIL	Hardware	CA Server	Comment
JCE	Dev	Unknown	Core 3.0.10	1-BCH	none	none
MHS ESO	Dev	Unknown	TBD	TBD	none	none
SMK G2	Dev	18.1.5	Core 3.0.10	TBD	TBD	none
SARATOGA	Live	17.1	Core 3.0.10	TBD	TBD	none
MUSCULAR	Live	18.1.1	18.1.5	TBD	TBD	none
SMK	Live	17.1	Core 3.0.10	TBD	TBD	none
CROSSCUT	Live	15.6.1	Core 3.0.10	TBD	TBD	none
MHS	Live	15.6.1	Core 3.0.10	TBD	TBD	none
TEC	Live	15.6.1	15.6.1	TBD	TBD	none

(U//FOUO) Monitoring

- (U//FOUO) CA servers are monitored by the T3332 Data Operations Center (DOC)as part of their TU monitoring (SLACKKEY) DOC TU SlackKey Homepage. To access the TopView TU ORC – DOC [redacted]
- (U//FOUO) The VALIANTSURF SOP used by the DOC VALIANT SURF Tab Special Instructions
- (U//FOUO) During business hours, the DOC uses the following contact list: DOC business hours POC list#VALIANTSURF
- (U//FOUO) DOC After Hours Call-in Procedures
- (U//FOUO) VALIANTSURF CA Server Troubleshooting Guide

(U) Governance

(U) DNC Thread Schedules

(U) VALIANTSURF Thread Status Weekly Meetings 2012

(U//FOUO) VALIANTSURF Activity Leads Status Review

(S//SI//REL) The VALIANTSURF Leads Meeting reviews are held weekly on Mondays. The purpose of this review is to discuss the major goals and status of activities taking place. Any roadblocks that would cause a failure in meeting the established goals should be discussed at this time.

(U) Team Members

- (U) [redacted]/S31322 Thread Lead
- (U) [redacted]/R1,IDA/CCS(CON) Architecture Lead
- (U) [redacted]/S31322(Integree) Architecture Team
- (U) [redacted]/S31322 Architecture Team
- (U) [redacted]/S31322(CON) Systems Engineer
- (U) [redacted]/S31322 Systems Engineer
- (U) [redacted]/S31322 Systems Engineer
- (U) [redacted]/S31322 SW Developer
- (U) [redacted]/S31322 SW Developer
- (U) [redacted]/S31322 SW Developer
- (U) [redacted]/S31322 SW Developer
- (U) [redacted]/S31322(CON) SW Developer
- (U) [redacted]/S31322(CON) SW Developer
- (U) [redacted]/S31322 SW Developer
- (U) [redacted]/S31322(CON) CAS Deployment
- (U) [redacted]/S31322(CON) Integration & Test Lead
- (U) [redacted]/S31322(CON) Integration & Test Engineer
- (U) [redacted]/S31322(CON) Integration & Test Engineer
- (U) [redacted]/S31322(CON) Integration & Test Engineer

- (U) [redacted]/S31322(CON) Integration & Test Engineer

Team Alias: DL Valiantsurf (mailto:[redacted]

(U) Stakeholders

- (U) [redacted]/S3124
- (U) [redacted]/T11
- (U) [redacted]/S313
- (U) [redacted]/T112
- (U) [redacted]S31243
- (U) [redacted]/S3124
- (U) [redacted]/S313
- (U) [redacted]/NCSC

weekly

(U) VALIANTSURF Historical –

(U//FOUO) Deployment Documents

- (S//SI//REL) Spin 11/12 Metadata Flow management
- (U) Spin 9 VPN PIQ Blade Version Description Document (VDD) for MHS, YRS, TEC
- (U) Spin 9 MHS PIQ Blade Baseline Change Request
- (U) Spin 8 VPN TML Test Checklist 20070416
- (U) Spin 8 VPN MHS Checklist 20070416

(U) Design Reviews and Technical Exchanges

- (S//SI//REL) VPN TU IT meeting minutes 1 May 2009
- (S//SI//REL) VPN/TUMMS requirements meeting minutes 23 April 2009
- (S//SI//REL) VPN TUBE Metadata Bundle Classification meeting minutes 3 April 2009
- (S//SI//REL) Brief to YRS during TDY 17–21 Nov 2008
- (S//SI//REL) Spin 12 TURBULENCE VPN Technical Review
- (S//SI//REL) Spin 10 TURBULENCE VPN Technical Review Minutes
- (S//SI//REL) Spin 10 TURBULENCE VPN Technical Review
- (S//SI//REL) Spin 10 VPN / ISLANDTRANSPORT / ISLANDHIDEAWAY Technical Exchange 20080124 Meeting Minutes
- (S//SI//REL) Spin 10 VPN / ISLANDTRANSPORT / ISLANDHIDEAWAY Technical Exchange 20080124 Meeting Agenda
- (S//SI//REL) Spin 9 TURBULENCE VPN Design Review
- (S//SI//REL) Spin 9 TURMOIL VPN Design Review Minutes
- (S//SI//REL) Spin 9 TURBULENCE VPN Design Review Minutes

(U//FOUO) VALIANTSURF Activity Leads Status Review

(S//SI//REL) The VALIANTSURF Activity Leads Status reviews are held bi-weekly on Mondays throughout the Spin. The purpose of this review is to discuss the major goals and status of activities taking place. Any roadblocks that would cause a failure in meeting the established goals should be discussed at this time.

(U) VPN Thread Schedules

- (U//FOUO) Spin 11 VPN Sprint Schedule
- (U//FOUO) Spin 10 VPN Sprint Schedule

(U) Pages of Interest

- (U//FOUO) TURMOIL VALIANTSURF
- (U//FOUO) TURMOIL GALLANTWAVE

Retrieved from '[redacted]
Category: VPN